D3

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2001-268071A**

(43)Date of publication of application : **28.09.2001**

(51)Int.Cl. **H04L 9/10**

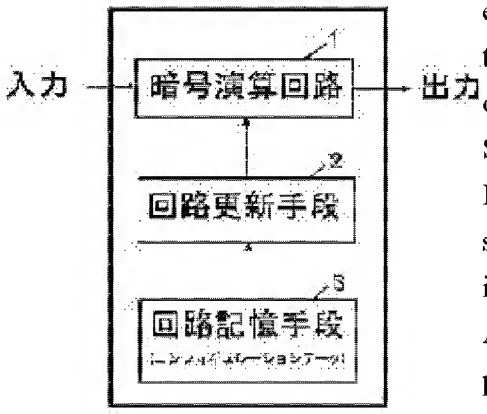
(21)Application number : **2000-074177**

(22)Date of filing : **16.03.2000**

(71)Applicant : **ADVANCED MOBILE TELECOMMUNICATIONS SECURITY TECHNOLOGY RESEARCH LAB CO LTD**

(72)Inventor : **ITO SATORU**

(54) ANTI-TAMPER ENCRYPTION DEVICE



(57)Abstract:

PROBLEM TO BE SOLVED: To provide an anti-tamper encryption device having the enhanced recurity by disenabling the analysis of contents even when fluctuation pattern of operating power of the encryption device is observed.

SOLUTION: An encryption arithmetic circuit 1 consists of an FPGA/PLD on an SRAM/flash memory basis. A circuit storage means 3 stores a plurality of configuration data that indicate the same function with different internal operations. A circuit update means 2 reads the configuration data in prescribed timing and writes the data to the encryption arithmetic circuit 1. Since the internal operation differs from each other according to the configuration data, a fluctuation pattern of the operation power differs from each other according to the configuration data. Even when the fluctuation of power consumption is observed, it is difficult to estimate the internal encryption processing so as to enhance the anti-tamper performance.

Detailed Descriptions of the Invention:

.....

[0008] Fig. 1 is a functional block diagram of an anti-tamper encryption device according to a first embodiment of the present invention. In Fig. 1, an encryption arithmetic circuit 1 is a circuit to execute encryption operation and decryption operation, which is constructed by a device capable of circuit reconfiguration. The device capable of circuit reconfiguration is not an anti-fuse that can execute configuration only once, but SRAM/flash memory-based FPGA/PLD capable of rewriting many times. For example, a product from Xilinx, Inc. or Altera Corporation may be used. Circuit update means 2 is means configured to write configuration data into the encryption arithmetic circuit. Circuit storage means 3 is storage means configured to retain configuration data.

.....